UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

INFORMATION ASSOCIATED WITH A CELLULAR DEVICE THAT IS IN THE CUSTODY OR CONTROL OF VERIZON

Case No. 1:23MJ239-1

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the _____ District of New Jersey , there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18USC§§1201(a)(1) & (c)	Kidnapping and conspiracy to commit the same
18USC§§1030(a)(2)(C),(4) & c	Unauthorized Access to a Computer and conspiracy to commit the same
18USC§§1956(a)(1)(B)(i) & (h)	Money Laundering and conspiracy to commit the same

The application is based on these facts:

See Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/Eric S. Nye
Applicant's signature

Eric S. Nye, Special Agent FBI
Printed name and title

On this day, the applicant appeared before me via reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Date: 6/8/2023 2:14 pm

Judge's signature

City and state: Durham, North Carolina

Joe L. Webster, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE CELLULAR DEVICE ASSIGNED TELEPHONE NUMBER (561) 707-2035 AND IMSI 311480649818812 THAT IS IN THE CUSTODY OR CONTROL OF VERIZON	Case No. 1:23MJ239-1

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, SA Eric Nye, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I am investigating a home invasion that involved kidnapping and the theft of a large amount of cryptocurrency in Durham, North Carolina on April 12, 2023. I make this affidavit in support of an application for a search warrant for location information associated with cellular telephone number **(561) 707-2035** and International Mobile Subscriber Identity (IMSI) 311480649818812 (hereinafter "Subject Telephone"), whose service is provided by Verizon, a wireless telephone service provider headquartered at 180 Washington Valley Road, Bedminster, New Jersey 07921.

2. The information sought by this application, which is acquired in the first instance by Verizon, is sought based on 18 U.S.C. § 2703(c)(1)(A). This warrant requires Verizon to disclose to the government copies of the information further described in Attachment B.

3. Specifically, authorization is sought to obtain historical location information related to the use of the Subject Telephone from March 15, 2023 through June 7, 2023, and prospective location information related to the use of the Subject Telephone for a period of 45 days from the date of this application, including: (1) information reflecting the location of cellular towers (cell-

site and sector/face) interacting with the Subject Telephone, including call detail, text, and data information ("Cell-site Information"), and (2) data collected by Verizon reflecting the physical location of the Subject Telephone, including network timing and geolocation information, for example Verizon's Periodic Location Updates and Real Time Tool (RTT), and all other records containing geolocation and timing advance measurements and distance-to-tower measurements for all technologies (CDMA2000, GSM, UMTS, LTE, 5G-NR) (collectively, "Phone Location Information"), along with any other associated data that was collected by Verizon, but not including the contents of any communication.

4. Because this warrant seeks the prospective collection of information, including cell-site location information, that may fall within the statutory definitions of information collected by a "pen register" and/or "trap and trace device," *see* 18 U.S.C. § 3127(3) & (4), the requested warrant is designed to also comply with the Pen Register Act. *See* 18 U.S.C. §§ 3121-3127. The requested warrant therefore includes all the information required to be included in an order pursuant to that statute. *See* 18 U.S.C. § 3123(b)(1).[1]

5. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18 U.S.C. §§ 1201(a)(1) and (c) (Kidnapping and conspiracy to commit the same), Title 18 U.S.C. §§ 1030(a)(2)(C), (4), and (c) (Unauthorized Access to a Computer and conspiracy to commit the same), Title 18 U.S.C. §§ 1956(a)(1)(B)(i) and (h) (Money Laundering

---

[1] The government complies with 18 U.S.C. § 3122(a)(1) by providing the required certification by the attorney for the government at the end of this application.

and conspiracy to commit the same) have been committed by REMY ST. FELIX, ELMER CASTRO, and JAROD SEEMUNGAL. Further, there is probable cause to believe that the location information described in Attachment B will constitute or lead to evidence, contraband, or fruits of these criminal violations.

AGENT BACKGROUND & KNOWLEDGE

7. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed since 2006. I have authored, executed, and/or participated in over a hundred search and seizure warrants for illegal narcotics and related paraphernalia. I have participated in the operation and execution of over thirty Federal and State Title III orders. I have arrested and/or participated in the arrest of over a hundred persons for violations of State and Federal narcotics statutes. I am currently assigned to investigate violent gangs in the Durham metropolitan area as a member of the FBI's Raleigh-Durham Safe Streets Task Force (RDSSTF) and have received over a hundred hours of specialized training in the area of illegal narcotics and violent street gangs. I have investigated firearm offenses, robberies, carjackings, kidnappings, and murders.

8. Through instruction and my participation in investigations, I have become familiar with the manner in which gang members and narcotics traffickers conduct their illegal business, and the methods, language, and terms that they use to disguise conversations about their gang and narcotics activities. Additionally, I have become familiar with gang members' methods of operation, including gang organizational structure, their methods of violence, their distribution, storage, and transportation of narcotics, and how they obtain and transport firearms.

9. During the course of the current investigation, I have consulted with members of the FBI's Cyber Squad who have extensive experience and training in online account compromises and cryptocurrency.

JURISDICTION

10. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. § 2703(c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

CELLULAR TELEPHONE COMPANIES

11. Cellular telephone companies routinely create and maintain, in the regular course of their business, records of information concerning their customers' usage of particular cell towers. For each communication a customer makes or receives, these records typically include (1) the date and time of the communication; (2) the telephone numbers involved; (3) the cell tower and sector to which the customer connected at the beginning of the communication; and (4) the duration of the communication. Cell-site Information is useful to law enforcement because of the information it provides about the general location of a cell phone when a communication is made.

12. Cellular telephone companies also routinely create and maintain, in the regular course of their business, records of information concerning their customers' usage that includes data reflecting the physical location of the phones themselves. Cellular telephone companies are required by the Federal Communications Commission to be able to provide latitude, longitude, and altitude information for telephones that call 911. This information is referred to as E-911 Phase II information. Cellular providers have been required to provide some form of E-911 data since approximately 1999, before the rollout of 3G cellular networks in the United States. Historically, cellular providers relied on Global Positioning System (GPS) capabilities for the location information. Cellular providers could, in response to a warrant, query a phone on their network about its location and receive location information from the handset.

13. Cellular providers are now able to determine the approximate (i.e., with an error radius) latitude and longitude of phones connected to their networks based on routine signaling information between the phones and the network towers. With respect to Verizon and AT&T, no query to the phone is necessary for the provider to collect this location information. Indeed, that information is collected simply by the fact of the phone being connected to the network and is a necessary part of the phone's operation on the cellular provider's network. This data is collected in the ordinary course of the provider's business. Cellular providers use a variety of terms to refer to this geolocation and network timing advance or distance-to-tower information, including Verizon's Periodic Location Updates and Real Time Tool and AT&T's Mobile Locator Tool and Location Database of Record. Carriers are therefore able to provide this data at regular intervals to law enforcement for both historical and prospective service.

BACKGROUND ON CRYPTOCURRENCY

14. Based on my training and experience, as well as my consultation with members of FBI's Cyber Squad, the following definitions and explanations apply to the activity discussed in the affidavit.

15. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency. Each unit of cryptocurrency is often referred to as a "coin" or "token." In general, most cryptocurrencies are considered fungible assets. Examples of cryptocurrency are Bitcoin, Ether, and Monero. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Users of cryptocurrency use public and private keys to transfer cryptocurrency from one person or place to another. A public key is typically a set of numbers and/or letters that a cryptocurrency user shares with other users

to engage in a transaction in cryptocurrency, whereas a private key is typically a set of numbers and/or letters that the user of an account maintains privately to access his or her cryptocurrency. A public key, or address, is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key"). A public address is represented as a case-sensitive string of letters and numbers. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

16. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[2] Although many cryptocurrencies are or purport to be pseudonymous, often law enforcement and currency exchangers can use the blockchain to analyze transactions in cryptocurrency, identify individuals who are using

---

[2] Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions. These are often referred to as "privacy coins." Monero is one example.

cryptocurrency platforms for illicit purposes, and trace fraud proceeds from victims to one or more exchanges or wallets. Cryptocurrency is not illegal in the United States.

17. Cryptocurrency is stored in a virtual account called a wallet, which can exist in, among other forms, an external computer device, a computer, on an application, online, or in devices designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. Access to a wallet and the cryptocurrency therein is typically protected by a password only known to the owner or user of the wallet. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Wallets can be either "custodial" or "non-custodial" (also referred to as "centralized" or "decentralized"). In the case of a non-custodial wallet, the owner of the wallet has sole control of the wallet's private keys, which enable access to the wallet and any funds contained therein. With a custodial wallet, another party controls the private keys to the wallet. This is usually a cryptocurrency exchange, and the relationship between the exchange and the customer can be considered analogous to the relationship between a traditional bank and its customers, where the bank securely maintains funds deposited by a bank customer.

18. Virtual currency "exchangers" and "exchanges", such as Binance and Coinbase, are individuals or companies that exchange virtual currency for other currencies, including U.S. dollars. Exchanges facilitate the purchase, sale, and transfer of a variety of digital currencies. Centralized exchanges generally maintain a custodial role for the wallets of its customers, and function as trusted intermediaries in cryptocurrency transactions. Decentralized exchanges consist of peer-to-peer marketplaces where users can trade cryptocurrencies in a non-custodial manner,

without the need for an intermediary to facilitate the transfer and custody of funds. Decentralized exchanges are often used to trade, or "swap", one type of cryptocurrency for another, for which the user pays a transaction fee. Centralized exchanges that conduct business in the United States are required to verify their customers' identities and abide by Know-Your-Customer/Anti-Money Laundering (KYC/AML) regulations. Currently, decentralized exchanges are generally not required to abide by KYC/AML regulations, as they do not take custody of funds and are merely providing a platform to facilitate trades between individual users.

19. Take Bitcoin[3] ("BTC"), a type of cryptocurrency, for example. Payments or transfers of value made with bitcoin are recorded in the Bitcoin blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire bitcoin through exchanges, bitcoin ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by "mining." An individual can "mine" bitcoins by using his or her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. As of May 23, 2023, one bitcoin is worth approximately $27,270.30 in U.S. dollars, though the value of bitcoin is generally much more volatile than that of fiat currencies.

20. Although cryptocurrencies such as bitcoin have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes, such as money laundering, and is an oft-used means of payment for illegal goods and services on hidden services websites

---

[3] Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

operating on the Tor network[4]. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track purchases within the dark web marketplaces

PROBABLE CAUSE

Armed Home Invasion at 1020 Wells St, Durham, NC on April 12, 2023

21. On April 12, 2023, at approximately 9:17am, the Durham Police Department responded to a report of an armed robbery at a residence on Wells Street in Durham, North Carolina (the Residence). A married couple (referred to hereafter as the Husband and the Wife), both seventy-six years of age, reside at the Residence. At approximately 7:30am, two black men (suspected to be ELMER CASTRO and REMY ST. FELIX) came to the door of the residence. The men were dressed as construction workers wearing reflective vests. They claimed to be inspecting pipes for damage and told the Husband that they would be walking around the house. Soon thereafter the men knocked again, and the Wife answered. The men pushed their way into the Residence. The Wife struggled and screamed causing the Husband to respond to her location. The men restrained and zip tied the Husband's hands and the Wife's hands. Both men were armed with handguns. The wife was dragged by the legs into a bathroom and detained by the smaller of the two men (Perpetrator-1). The Husband was forced at gunpoint to the rear of the Residence and up to a loft home office by the larger of the two men (Perpetrator-2).

---

[4] Tor, short for "The Onion Router," is free and open-source software for enabling anonymous communication. It directs Internet traffic via a free, worldwide, volunteer overlay network that consists of more than seven thousand relays. It protects the user's freedom and ability to communicate confidentially through IP address anonymity using Tor exit nodes

22. Perpetrator-2 forced the Husband to login[5] to his Apple iMac and then into his Coinbase account, a custodial cryptocurrency exchange based in the United States. Perpetrator-2 then took over control of the iMac. Perpetrator-2 was on a call with a third individual (Perpetrator-3), believed to be JAROD SEEMUNGAL, and was using the speaker on his phone. Perpetrator-3 provided Perpetrator-2 instructions about how to transfer cryptocurrency from the Husband's Coinbase account. Husband described Perpetrator-3 as tech savvy. Perpetrator-3 knew details about the account without being told. Based on my training and experience this shows that an account belonging to the Husband had been previously compromised (believed to be Husband's email). Investigators subsequently determined that, over a period of approximately forty-five minutes, $156,853 worth of cryptocurrency was transferred out of Husband's Coinbase account in three transactions. A fourth transaction was denied. The Husband described Perpetrator-2 as very threatening. Perpetrator-2 threatened to cut off Husband's toes and genitalia, to shoot him, and to rape his wife if he didn't access his Coinbase account. Perpetrator-2 was wearing khaki cargo pants and a black hat with a trout on it that said "Trout Pro Shop." He was armed with a black semiautomatic handgun.

23. Perpetrator-1 was wearing all black and a ski mask with a face covering. Perpetrator-1 was armed with a revolver with a subdued pink cylinder. He showed the Wife that it was loaded by opening the cylinder. Perpetrator-1 told the Wife that she had a "small bed for people with money." While Perpetrator-1 detained the Wife in the bathroom, he replaced the zip

---

[5] Perpetrator-2 cut the zip tie on Husband's hands so that he could type.

tie on her hands with a looser zip tie at her request.[6] The men attempted to duct tape the Wife's mouth shut.

24. The men destroyed the Husband's iMac and the couple's phones by smashing them. They put the Husband in the bathroom with the Wife, threatened them, and then left. The Husband and Wife left the Residence and made contact with their neighbors.

25. Durham Police Department officers canvassed the neighborhood for video. They located surveillance video from a nearby house depicting a BMW X5 SUV conducting what appears to be surveillance on the Residence on each of the three days prior to the robbery. On the day of the robbery, surveillance video showed the BMW park on the street in front of the Residence at approximately 7:28am and leave the residence at approximately 9:07am. The below are images taken from surveillance video of the BMW.

26. With assistance from BMW, investigators were able to identify the SUV as a 2019-2023 BMW X5, 45e, with chrome trim, roof rails, and 20-inch wheels. The color is either arctic grey metallic or dark graphite metallic.

---

[6] The Wife was able to remove her hands from the zip tie.

Evidence of an Account Compromise

27. The Husband explained that in the months preceding the robbery, he received multiple notifications to his phone that both his email account and Coinbase account passwords had been changed. The Husband did not change the passwords. When the Husband would attempt to gain access to those accounts, his passwords were no longer valid. The Husband would change the password and successfully gain access back to those accounts. Logs from the Husband's Coinbase account show multiple successful changes to the Husband's Coinbase password via IP addresses not used by the Husband. Based on my training and experience, and conversations with agents who investigate cybercrimes, I know that the circumstances that the Husband has reported are consistent with account takeovers. Husband used a multifactor authentication application for his Coinbase account thereby preventing anyone without access to the application from accessing his Coinbase account, even if they knew the password. Husband's Coinbase account was registered to his email account and consequently sent communications regarding the Coinbase account to the email account. Based on these facts and the private information that Perpetrator-3 knew about Husband's Coinbase account, I believe that Husband's email was accessed without authorization and the perpetrator attempted to access Husband's Coinbase account without success.

Tracing of Stolen Funds

28. Investigators obtained records from cryptocurrency exchanges Coinbase and FixedFloat and examined public blockchain to determine the path of the stolen funds. As explained below, investigators traced stolen funds to accounts owned by REMI ST. FELIX and ELMER CASTRO of West Palm Beach, Florida. Both men received $22,267 of the Husband's stolen

cryptocurrency. Further, investigators traced stolen funds to a Coinbase account owned by JAROD SEEMUNGAL. The following is a timeline outlining the path of the stolen cryptocurrency:

April 12, 2023 – Day of the Home Invasion

a. 8:13am - Coinbase records show that the victim's account was accessed (login conducted by the Husband at gunpoint).

b. 8:14-8:20am - The perpetrators converted multiple of Husband's cryptocurrency holdings into Ether cryptocurrency coins (ETH)[7].

c. 8:23am - The perpetrators transferred 7.49386854 ETH, worth approximately $14,037, to wallet 0x9CE61b21705c0e24666f6aBcbd75c56a15E80759 (hereinafter referred to as "0x9CE61b").

d. 8:26-8:32am - The perpetrators exchanged cryptocurrency for USD Coin (USDC)[8].

e. 8:40am - The perpetrators transferred 4.63376598 BTC, worth approximately $140,619, to wallet bc1qphezmdc0l009y6fzn68khdwv45tvun0wxd4r98.

f. 8:42am - The perpetrators again converted multiple of Husband's cryptocurrency holdings into ETH.

g. 8:48am - The perpetrators transferred 1.16478113 ETH, worth approximately $2,197, to wallet 0x9CE61b.

h. 8:50am - The perpetrators again converted multiple of Husband's cryptocurrency holdings into ETH.

i. 9:01am - The perpetrators attempted, but failed, to transfer 4.73712395 ETH, worth approximately $9,144.83, to wallet 0x9CE61b.

---

[7] Ether is the cryptocurrency used by the Ethereum platform. Transactions in Ether are categorized as pseudo-anonymous since tracing the identity of an Ethereum wallet owner or receiver of funds requires extensive chain analysis and data mining.

[8] USD Coin can always be redeemed for $1.00 giving it a stable price. It is a type of coin referred to as a stablecoin.

29. The above successful transfers of funds were first sent to unhosted wallets[9] before ending up at the cryptocurrency exchange FixedFloat[10] to be swapped into Monero[11] (XMR), a privacy coin.

April 12, 2023 – Day of the Home Invasion

a. 9:41am-10:10am - The perpetrators transferred all cryptocurrency into XMR.[12] Some of these transfers were conducted in a unique FixedFloat session identified as 4772292 allowing the funds to be connected to subsequent transfers in the same session.

b. 10:57-11:40am - In FixedFloat session 4772292, the perpetrators placed orders to FixedFloat to exchange XMR coins into ETH and BTC. These transactions[13], although "untraceable" on a public blockchain as they were sent to FixedFloat's

---

[9] An unhosted wallet is not hosted by a third-party financial system. It can be very difficult or impossible to determine who is accessing or in control of the use of cryptocurrencies in an unhosted wallet. Unhosted wallets allow for anonymity and concealment of illicit financial activity.

[10] According to its website, "FixedFloat is a fully automated service for exchanging cryptocurrencies and tokens on favorable terms. FixedFloat is not custodial. The exchange takes place immediately after receiving the coins and the required number of network confirmations."

[11] Monero is a cryptocurrency which uses a blockchain with privacy-enhancing technologies to obfuscate transactions to achieve anonymity and fungibility. Observers cannot decipher addresses trading Monero, transaction amounts, address balances, or transaction histories.

[12] FixedFloat session 4772292 received order M2MVM5 to exchange 4.327 ETH for 50.589 XMR. FixedFloat session 4772987 received order HH3J1D to exchange 2.316 BTC for 426.575 XMR. FixedFloat session 4772987 received order ZCVBUC to exchange 4.327 ETH for 51.037 XMR. FixedFloat session 4772292 received order 15GTBM to exchange 1 BTC for 185.121 XMR. FixedFloat session 4772292 received order 8D13M2 to exchange 1.316 BTC for 244.153 XMR.

[13] FixedFloat session 4772292 received order 9GQ2E3 to exchange 282.649 XMR for 23.419 ETH (destination ETH address: 0xd82b9df48AC6dce3860fBDE2D0fa29C74c2A0438). FixedFloat session 4772292 received order H45Q38 to exchange 2 XMR for .166 ETH (destination ETH address: 0x9BD7fC87ad035632E4A4a1d4Cc3C41f05779e0A6). FixedFloat session 4772292 received order S6G557 to exchange 44.05765296 XMR for . 0.23583427 BTC (destination BTC address: bc1qerl7jlnuwp3435jf8937f2gqztamjz0xx3y2qn).

public deposit address, were recorded by FixedFloat as having been executed by the same computer and logged by FixedFloat during the same session, 4772292. This was determined by cookie[14] logs indicating that the same browser, and therefore the same user, had conducted these transactions.

30. Approximately 90 minutes after the home invasion, at 11:42am, a Coinbase account was opened in the name ELMER CASTRO, account 6436d16b68c1b8102da3cc29. In order to open the account, the user provided an image of the front and back of CASTRO's Florida driver's license. The account was registered to phone number 561-836-3039, email lile561@icloud.com, and address 5930 Elmhurst, West Palm Beach, Florida.

31. Approximately eight hours after the home invasion, at 5:04pm, a Coinbase account was opened in the name REMY RA ST. FELIX, account 64371cd3fc40f11ff8620813. In order to open the account, the user provided an image of the front and back of ST. FELIX's Florida driver's license. The account was registered to phone number 561-660-3482, email remgodbooking@gmail.com, and address 1656 Barbie Ln, West Palm Beach, Florida. The account was opened from a mobile device utilizing an IP address registered in North Carolina.

32. Additionally, Coinbase records revealed account, 6091bd9774c75e02ee8aad14, had previously been opened with the same user provided identifiers for REMY ST.FELIX but registered to remdem9@icloud.com and phone number 561-856-4777.

33. Coinbase records revealed that JAROD SEEMUNGAL already had two Coinbase accounts on the day of the robbery. For both accounts, the user provided an image of the front and

---

[14] Cookies, as defined by Microsoft, are small files that websites put on your computer or device to store info about your preferences. Cookies can improve your browsing experience by allowing sites to remember your preferences or by letting you avoid signing in each time you visit certain sites.

back of SEEMUNGAL's Florida driver's license, SEEMUNGAL's social security number, and phone number **561-707-2035 (Subject Telephone)**. Coinbase account 591b8f3cee2435024475aba1 was opened in May 2017 and is registered to email thedarkswallows@gmail.com and address 1861 Meadow Court, West Palm Beach, FL 33406.[15] Coinbase account 5d13ff3es2227b04f84db56a was opened in June 2019 and is registered to email jarod.s@outlook.com and address 4144 Palm Bay Circle, West Palm Beach, FL 33406

April 12, 2023 – Day of the Home Invasion

a. 10:57am - FixedFloat Order ID 9GQ2E3 swapped 282.64911865 XMR of stolen funds, worth approximately $44,296.91, into 23.4179441 ETH that was sent to 0xd82b9df48AC6dce3860fBDE2D0fa29C74c2A0438 (hereinafter referred to as "0xd82b9d").

b. 11:16am - The 23.4179441 ETH from address 00xd82b9d is swapped into USDC using the Uniswap[16] service.

c. 12:11pm - Wallet 0xBD97ADC972c4B96cECd0eA3F9923cd9Fe733E7A7 at CASTRO's Coinbase account (6436d16b68c1b8102da3cc29) received 22,267 USDC, worth $22,267, of stolen funds.

d. 12:13-12:31pm - The full amount of USDC in CASTRO's Coinbase account was sold and withdrawn to Wells Fargo bank account ******4336 in the name ELMER CASTRO.

---

[15] Both the name Jarod Seemungal and Jarod Lastierre are listed on the account's subscriber information.

[16] Uniswap is a decentralized cryptocurrency exchange that uses a set of smart contracts to execute trades on its exchange. It's an open-source project and falls into the category of a Decentralized Finance product because it uses smart contracts to facilitate trades. Smart contracts are scripts that automate the actions specific to a contract between two parties. Smart contracts do not contain legal language, terms, or agreements, only code that executes actions when specified conditions are met.

April 13, 2023 – Day After the Home Invasion

e. 12:35pm - Wallet 0xF204af1F33AF212b20298822d449adEba33616F0 at ST. FELIX's Coinbase account (64371cd3fc40f11ff8620813) received 22,267 USDC, worth $22,267, of stolen funds, the same amount received by CASTRO.

f. 13:45pm - $5,000 worth of the USDC in ST. FELIX's Coinbase account was sold and withdrawn to Stride bank account ******3085 in the name REMY ST. FELIX.

April 15, 2023

g. 12:37am - FixedFloat session 4772292 received order 4ZU8KN to exchange 4.194 XMR for 0.02226636 BTC, worth approximately $677.41. The BTC was sent to address bc1qdg4nl3md96nnqwflcsleyvsm5cm0jx0xdp4jc6.

h. 10:27pm - FixedFloat session 4772292 received order VKDSCG to exchange 4.199 XMR worth of stolen funds for 0.3226519 ETH, worth approximately $678.09. The ETH was sent to address 0x5811724395e47aBaDC5f82909d509F70Df2f0512 (hereinafter referred to as "0x581172") at Binance, a custodial cryptocurrency exchange. The Binance account, user ID 147169368, is registered to Alexander Birch with e-mail alexander.birch@email.com. Binance records show that an Apple device with the name "jarod" logged into the account.

April 18, 2023

i. 9:57am - FixedFloat session 4772292 received order K3H4A7 to exchange .334 stolen ETH to 7484.3 DOGE[17], worth approximately $664.49. The DOGE was sent to address DTVUxBMXzP2M5va1SsYRNqHT4ciANDtSoD (hereinafter referred to as "DTVUxBMX").

j. 10:09am - SEEMUNGAL's Coinbase account (591b8f3cee2435024475aba1) DOGE wallet received 7484.281 DOGE from the address DTVUxBMX. The DOGE was sent to address DSUbtSBba9QDyKyYvhs2DrV3rMthu6pc8a.

April 19, 2023

---

[17] Dogecoin (DOGE) is a novelty cryptocurrency originally launched as a "memecoin" (inspired by an image, video, piece of text, etc., typically humorous in nature, that is copied and spread rapidly by internet users, often with slight variations) within the cryptocurrency community. Over time, however, Dogecoin has grown into a large blockchain network and is one of the most popular altcoins available in the market.

k. 12:15pm - $2,500 worth of the USDC in ST. FELIX's Coinbase account was sold and withdrawn to Stride bank account ******3085.

34. On May 1, 2023, SEEMUNGAL's Coinbase account (591b8f3cee2435024475aba1) sent ETH to wallet 0x581172 belonging to Binance user ID 147169368 on two separate occasions.

35. Having reviewed the above-documented information and had discussions with the FBI cryptocurrency investigators that mapped this data, I believe that JAROD SEEMUNGAL, REMY ST. FELIX, ELMER CASTRO, and others yet identified, possessed the stolen cryptocurrency immediately following the armed home invasion.

Cell Tower Data and Mapping

36. A North Carolina Superior Court Judge authorized investigators to obtain records from cellular network providers identifying the devices that used cell towers providing coverage to the Residence on April 11, 2023 between 5:56 am and 7:30 am and on April 12, 2023 between 7:30 am and 9:07 am. AT&T records showed that phone numbers 561-836-3039 and 561-660-3482 both used cell towers that provided coverage to the Residence within the listed time frames on both days. As described about, these phone numbers are registered, respectively, to the Coinbase accounts of CASTRO and ST. FELIX.

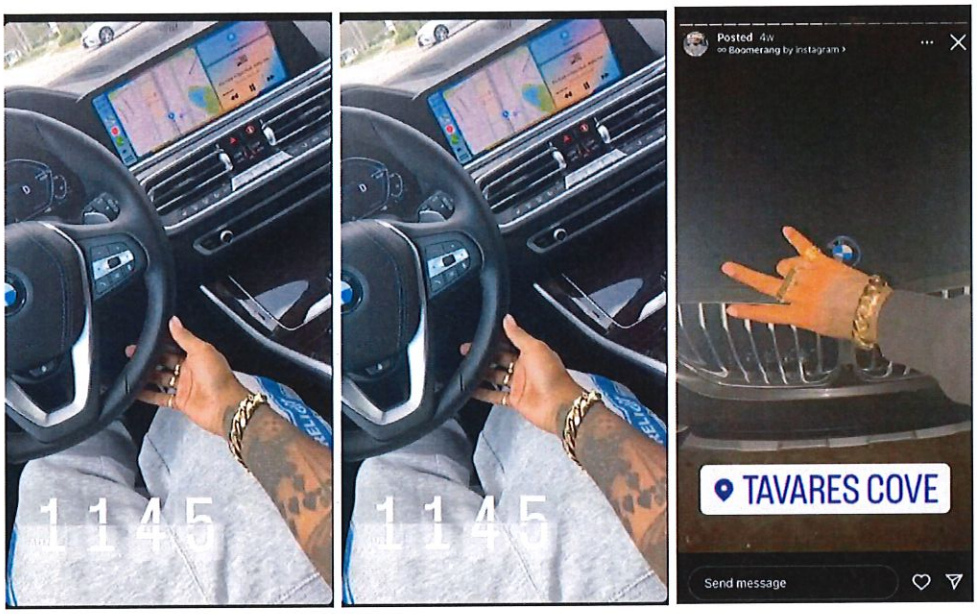
37. CASTRO and ST. FELIX reside in West Palm Beach, Florida.

Review of Social Media Accounts

38. Investigators with the Palm Beach County Sheriff's Office were able to view the Instagram account e_murda561. The account belongs to ELMER CASTRO as evidence by the

users tattoos and jewelry. Specifically, a rap music video depicting CASTRO shows his jewelry and tattoos. The user of the Instagram account has matching jewelry and tattoos.

39. A saved story on the account from around the time of the home invasion depicted CASTRO driving in a BMW X5 which was consistent with the color of the BMW used during the home invasion. Below are images taken from that story:



Evidence of Similar Previous Conduct by JAROD SEEMUNGAL

40. Between March 1, 2021, and March 3, 2021, a BlockFi exchange account was remotely taken over and the funds stolen. The matter was investigated by FBI Newark. The investigators determined that the victim's account was illegally accessed without authorization and that 28.26 Bitcoin and 1,096 Ethereum, totaling approximately $3.5 Million at the time, were taken from the victim located in Delray Beach, Florida.

41. On September 11, 2022, this same victim was victimized again during an armed home invasion by three males. The individuals demanded that the victim give them passwords for

her laptop and cryptocurrency accounts. The victim declined and the suspects fled, but took the victim's electronic items, including cell phones and a laptop.

42. Investigators obtained records from Bitpay, a cryptocurrency payment service provider, related to transactions made by SEEMUNGAL. A BitPay transaction registered to JAROD SEEMUNGAL involved the transmission of 2.719079 Bitcoin (worth approximately $138,158 at the time) to a car dealership and auto-auction business.[18] The transaction identified SEEMUNGAL by his date of birth, license number, and social security number. The email address provided jarod@null.net and the physical address was 50 Biscayne Blvd #912, Miami, Florida, Bitpay flagged the transaction as suspicious. The transaction was executed on March 3, 2021 from IP address 96.69.39.209. The payment originated from BTC address bc1qw7zew6xjfvszq8fmdhg69za306rkkkadz5qe2u (hereinafter referred to as "bc1qw7"), presumed to be controlled by SEEMUNGAL given the information collected by Bitpay.

43. Investigators were able to trace back a portion of the funds received by address bc1qw7 to a portion of the money stolen from the Delray Beach victim's BlockFi account. In summary, investigators were able to track a portion of the stolen funds from the Delray Beach victim to SEEMUNGAL's BTC address, bc1qw7 and the described Bitpay transaction.

44. Further, a review of the deposit activity of address bc1qw7 revealed indirect exposure[19] to two known fraud sites, AlphaBay and Dream Market, and to a gambling service

---

[18] BitPay requires proof of identification from shoppers for all transactions equal to or above $3,000.

[19] "Exposure" is defined as the relationship between an address and other entities that is created through the transfers made to and from that address to other entities. Exposure may be "direct",

known as Bustabit. Address bc1qw7 had indirect exposure to the BTC address bc1qykhkn5w2ch6gjgse4a04yxas2nps0gwfzfns2d, which was used by the Bustabit user "MeowlolMeow". Other BTC addresses controlled by the Bustabit user MeowlolMeow had direct exposure to receiving 13.9934 BTC that were marked as "Stolen Funds" in Chainalysis Reactor.[20] These funds originated from the BTC address bc1qdjkc4e3u8jup6axtda560z720vapq5p34pmwgu which is an address that received stolen funds from the BlockFi account takeover of the victim in Delray Beach, Florida.

The Subject Telephone

45. Verizon provides service to the cellular telephone number **(561) 707-2035** and International Mobile Subscriber Identity (IMSI) 311480649818812 ("Subject Telephone"). Verizon records reveal that the Subject Telephone is subscribed to JAROD SEEMUNGAL at email jarod.s@outlook.com and address 4144 Palm Bay Circle, West Palm Beach, FL 33406

CONCLUSION

46. I seek prospective information and, to an extent, historical information via this application because this information will assist me in gathering evidence in the ongoing investigation that I have described above in the following ways: (1) I am investigating a conspiracy, and determining concert of action and contact between the conspirators is of value to

---

meaning the funds came or went directly from a specific entity or address, or "indirect", meaning there are one or more steps between the entity or address.

[20] The Chainalysis Reactor service is used to connect cryptocurrency transactions to real-world entities and helps users examine criminal activity, such as the movement of stolen funds, as well as legitimate activity. Chainalysis designates a wide variety of services (e.g., exchanges, darknet markets, mixers, ATMs) and events (e.g., stolen funds, terrorist financing, scams) on the blockchain as exposure categories.

my investigation; (2) the information may enable me to identify members of the conspiracy that I have not previously identified; (3) the information will very likely identify locations where evidence (e.g., devices and their contents, clothing, guns, the BMW) and proceeds are stored and where search warrants may be appropriate. Moreover, it will assist in targeting surveillance conducted in this case, and reduce the risk of being detected and revealing the nature or fact of the investigation. People who are involved in criminal activity are often conscious of being followed and keep a close eye out for surveillance units. The chance of being discovered increases with the more surveillance that is done and the closer the surveillance units must get to the target subjects. Use of the prospective location information enables the investigative team to be more focused and judicious in its use of surveillance to those times when it appears that events of significance are going to occur. It also enables the investigative team the ability to conduct surveillance at a greater distance, because the fear of losing the target is reduced when surveillance is maintained via this information

47. I request that the Court issue the proposed search warrant pursuant to 18 U.S.C. § 2703(c)(1)(A).

48. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Verizon. Because the warrant will be served on Verizon, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

/s/Eric S. Nye

Eric S. Nye
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on June 8, 2023, 2:14 pm.

JOE L. WEBSTER
UNITED STATES MAGISTRATE JUDGE

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH ONE PHONE STORED AT PREMISES CONTROLLED BY VERIZON	Case. No. 1:23MJ239-1

ATTORNEY CERTIFICATION

The United States of America, moving by and through Eric L. Iverson, its undersigned counsel, respectfully submits under seal this attachment to the search warrant application by Federal Bureau of Investigation (FBI) Special Agent Eric Nye in the above-captioned matter. To the extent that cellular location information subject to the search warrant, specifically "dialing, routing, addressing, and signaling information" data inherent to the collection of cell-site location information falls within the scope of the Pen Register Act, 18 U.S.C. §§ 3121, et seq., this warrant also serves as an *ex parte* application for an order pursuant to 18 U.S.C. §§ 3122 and 3123, authorizing the installation and use of a pen register and trap and trace service on the cellular telephone described in Attachment A of the warrant (the "Subject Telephone"). In support of this application, the United States asserts:

1. This is an application, made under 18 U.S.C. § 3122(a)(1), for an order under 18 U.S.C. § 3123 authorizing the installation and use of pen register and a trap and trace devices.

2. The undersigned applicant is an "attorney for the government" as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure.

3. The law enforcement agency conducting the investigation is the Federal Bureau of Investigation (FBI).

4. The applicant hereby certifies that information likely to be obtained by the requested use of the technological equivalent of a pen register or trap and trace device is

relevant to an ongoing criminal investigation being conducted by the FBI as detailed in the above-captioned search warrant affidavit.

5. A "pen register" is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." 18 U.S.C. § 3127(3). A "trap and trace device" is "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." 18 U.S.C. § 3127(4). In the traditional telephone context, pen registers capture the destination phone numbers of outgoing calls, while trap and trace devices capture the phone numbers of incoming calls. Similar principles apply to other kinds of wire and electronic communications.

6. The technological equivalent of a pen register or trap and trace device sought by this application will record, decode, and/or capture dialing, routing, addressing, and signaling information associated with cell-site location data collected by Verizon, the cellular service provider for the Subject Telephone, anywhere within the United States.

7. The foregoing is based on information provided to me in my official capacity by agents of the FBI, including the warrant in the above-captioned matter.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on the 8th day of June, 2023.

Eric L. Iverson
Assistant United States Attorney

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with cellular telephone number (561) 707-2035 and International Mobile Subscriber Identity (IMSI) 311480649818812 (Subject Telephone) whose service is provided by Verizon, a wireless telephone service provider headquartered at 180 Washington Valley Road, Bedminster, New Jersey 07921.

ATTACHMENT B

Information to be Disclosed by Verizon

Verizon is required to disclose to the government (1) all information reflecting the location of cellular towers (cell-site and sector/face) interacting with the Subject Telephone, including call detail, text, and data information (Cell-site Information) and (2) all data collected by Verizon reflecting the physical location of the Subject Telephone, including network timing and geolocation information, including Verizon's Periodic Location Updates and Real Time Tool (RTT), and all other records containing geolocation and timing advance measurements and distance-to-tower measurements for all technologies (CDMA2000, GSM, UMTS, LTE, 5G-NR) (Phone Location Information) for the Subject Telephone gathered by Verizon from March 15, 2023 through June 7, 2023 (historical information) and from June 8, 2023 to July 23, 2023 (prospective information), along with any other associated data collected by Verizon, but not including the contents of any communication.